REMARKS

This paper is responsive to the non-final office action mailed on January 3, 2006 and to the personal interview held on May 11, 2006 at the U.S. PTO with the undersigned attorney of record.

SUBSTANCE OF INTERVIEW

Applicants' representative thanks Examiner Bhatia and Supervisory Examiner Cardone for the courtesies extended during the interview held on May 11, 2006. During the interview, Applicants' representative pointed out that the two primary references relied upon in rejecting the pending claims, TunnelBuilder for Mac User's Guide (MacTB) and TunnelBuilder 4.01 for Windows Website (WinTB) could not properly be combined as suggested, because the two references clearly teach away from each other. In particular, WinTB clearly states on page 1 that "SuperTunnel will only work between TunnelBuilder for Windows clients and TunnelMaster servers. It is not supported in the Macintosh version of TunnelBuilder." Examiner Bhatia suggested that this argument should be presented in this paper, which has been done below.

During the interview, Applicants' representative also spent time comparing independent claim 47 to the figures relied upon in the office action from MacTB, and in particular showing how numerous elements of this claim were not shown in either MacTB or WinTB, alone or in combination. For example, claim 47 recites two separate firewalls each associated with a separate computer. Examiner Bhatia asked whether the "return path" recited in the claims might be spelled out in more detail. Applicants' representative agreed to consider this possibility. As to dependent claim 49, Examiner Bhatia inquired as to whether it was clear that the intermediate server computer was located between the first and second computers, and Applicants' representative agreed to consider clarifying this dependent feature. Examiner Bhatia also mentioned the possibility that the claims could be amended to more particularly recite port 80 as the port that was used transmit messages. No agreement was reached.

DISCUSSION

Claims 1-2, 4-5, 7-8, 11-13, 15, 19-22, 24, and 26-56 were rejected as being obvious over the combination of MacTB in view of WinTB. According to the office action, it would have been obvious to combine the MacIntosh version of TunnelBuilder with the Windows version of TunnelBuilder because they are both made by the same company. However, as pointed out above, the two references clearly teach away from each other. In particular, WinTB clearly states on page 1 that "SuperTunnel <u>will only work</u> between TunnelBuilder for Windows clients and TunnelMaster servers. <u>It is not supported in the Macintosh version of TunnelBuilder.</u>" Moreover, there would be no motivation to combine two different incompatible products, each targeting a completely different (and incompatible) computer architecture. Accordingly, the rejections based on this combination should be withdrawn.

Even if the combination were proper, the proposed combination would not show all the claimed features. For example, as explained during the interview, independent claim 47 specifically recites two separate firewalls, each associated with a different computer, and recites specific messages traveling between the computers. Nowhere does MacTB or WinTB disclose these features. MacTB and WinTB merely disclose VPNs going through firewalls. For all embodiments except the "SuperTunnel" variant, it is evident that the firewalls must be specially configured rather than using a firewall port that is normally open to Internet traffic. This problem is even hinted at on page 1 of WinTB, which refers to "typical problems that you run into with VPN over firewalls or routers that don't support GRE packets to access your private network." As to the "return path" language of claim 47, the specification clearly explains this feature in paragraphs 34, 40, and 61 among other places. (Well-known stateful firewalls pass all outgoing TCP packets but will only allow incoming packets if they are part of an established connection, e.g., a "return path" that is created when a web server sends an acknowledgement packet in response to an outgoing message such as an HTTP POST message). The recited return path is not disclosed in the references as claimed.

Independent claim 1 has been slightly amended to more specifically recite that the HTTP message is transmitted through a firewall port that is normally open to HTTP packets to distinguish over other ports that may be used for other types of "Internet" packets (e.g., UDP). Corresponding minor amendments have been made to dependent claim 4.

As to dependent claim 2, page 4 of the office action suggests that it is inherent that "intermediate computers" on the Internet route packets without decrypting their contents. But claim 2 recites that "said server" transmits the encrypted message contents without decryption, and earlier the office action stated that the PPTP/L2PT server of MacTB corresponded to the "server" of the claim, which performs decryption of an encrypted identifier of the second computer. On page 3, the office action (in rejecting claim 1) relied on the PPTP/L2TP server of MacTB for disclosing <u>decryption</u> of the encrypted identification. This reliance on the MacTB PPTP/L2TP server to show the recited encryption as to claim 1 and other "intermediate" servers to avoid decryption of the message contents does not comport with the language of claim 2. In other words, independent claim 1 recites that the server decrypts an encrypted identifier of the second computer, and dependent claim 2 further recites that the server does not decrypt the contents of the message. The PPTP/L2TP server of MacTB performs decryption as pointed out in the office action.

As to dependent claim 12, which recites repeated transmissions from the first server in order to keep open a communication path, page 6 of the office action refers to page 3-17 of MacTB for this feature. But that page merely states that a connection will time-out after an inactivity period of 20 minutes. Nowhere is the recited repeated transmission step disclosed or suggested. Dependent claim 13 recites a similar feature that is not found in MacTB.

The arguments above also apply to independent claims 19, 21, 24, 26, 27, and 45 to the extent that their terms recite such features.

As to dependent claims 20 and 22, page 8 of the office action points to MacTB page 1-1 as showing the recited compression. No such feature is shown on page 1-1 of MacTB. To the contrary, WinTB clearly states on page 6 of 7 (website) that "Tunnelbuilder does not support compression."

As to dependent claim 49, the office action points to the PPTP/L2TP server of MacTB as disclosing the recited intermediate server computer. This claim has been amended (per the examiner's suggestion during the May 11 interview) to even more particularly state that the intermediate computer is located between the first and second firewalls. Given that MacTB only discloses a single firewall, this feature is clearly not shown.

As to dependent claim 50, which recites transmitting the encrypted message content via

the return path, no such feature is shown in MacTB.

As to dependent claim 51, which recites specific encryption and decryption steps, Applicants have carefully studied MacTB on the pages cited in the office action but cannot find any support for such a rejection.

As to dependent claims 52-54, Applicants have carefully studied MacTB on the pages indicated but cannot find any support for these rejections.

The office action rejects claims 55-56 without any further discussion. However, independent claim 55 recites 7 very specific steps that are nowhere to be found or suggested by MacTB or WinTB. Accordingly, the rejection of these claims should be withdrawn.

By this amendment, new independent claim 57 has been added. This claim specifically recites a method of communication between two computers each protected by a separate (and different) firewall, comprising specific steps including receiving an HTTP message from the first computer through a port that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic; from the third computer, sending a first response message to the first computer through the port in the first firewall, thereby establishing a first receive channel through the first firewall (see paragraph 61 of the specification, which clearly defines "receive channel"), wherein the first response message is linked to the first HTTP message; at the third computer, receiving a second encrypted HTTP message from the second computer through a port in the different second firewall that is configured to be open to outgoing HTTP traffic and open to incoming HTTP traffic that is responsive to and linked to outgoing HTTP traffic; from the third computer, sending a second response message to the second computer through the port in the different second firewall, thereby establishing a second receive channel through the second firewall, wherein the second response message is linked to the second HTTP message; at the third computer, receiving a third encrypted HTTP message from the first computer through the port in the first firewall; determining that the third encrypted HTTP message is intended to be delivered to the second computer, and transmitting to the second computer the third encrypted HTTP message, wherein the third encrypted HTTP message is transmitted over the second receive channel to the second computer; and from the third computer, periodically transmitting "keep alive" messages to the first and second computers to avoid a time-out condition. These features are not shown or

suggested by any of the cited prior art. New dependent claim 58 further recites that step (5) is performed at the third computer by transmitting the third encrypted HTTP message to the second computer without decrypting contents of the third encrypted HTTP message. Applicants can find no such suggestion in the art cited by the examiner.

If the Examiner believes that further discussion would expedite prosecution of this application, he is invited to contact the undersigned at the indicated telephone number.

Respectfully submitted,

By:_____

Bradley C. Wright
Reg. No. 38,061

BANNER & WITCOFF, LTD.
1001 G Street, N.W., 11th Floor
Washington, D.C. 20001
(202) 824-3160

Dated: June 5, 2006